Statement for the Record

James M. Chaparro

Deputy Assistant Secretary for Mission Integration

Office of Intelligence and Analysis

Department of Homeland Security

before the

Intelligence, Information Sharing and Terrorism Risk Assessment Subcommittee

of the Committee on Homeland Security

United States House of Representatives

July 26, 2007

Thank you Chairwoman Harman, Ranking Member Reichert, and Members of the Sub Committee. I am pleased that you have provided me with the opportunity to appear before your Committee to discuss our role in sharing intelligence with the private sector, and to discuss the lessons we have learned.

The Office of Intelligence and Analysis (I&A) is transforming the way that DHS performs its intelligence responsibilities. As you know, I&A has established five overarching and bold priorities to carry out this transformation. Each of these focus areas are designed to allow us to provide our customers with the highest quality intelligence available, to protect the homeland, and to serve as good stewards of the resources that the Congress has provided us to carry out our mission. Our priorities are:

- Improving the quality and timeliness of intelligence analysis across the Department;
- Integrating DHS Intelligence across its several components;
- Strengthening our support to state, local, and tribal authorities, as well as to the private sector;
- Ensuring that DHS Intelligence takes its full place in the Intelligence Community; and,
- Solidifying our relationship with Congress by improving our transparency and responsiveness.

The Threats are Real and Our Work is Important:

Just last week, the Director of National Intelligence released a national intelligence estimate (NIE) that described the nature of the threat that we face in the Homeland. An NIE represents the Intelligence Community's most authoritative views on national security issues, is the product of extensive research and coordination, and involves the work of the best and brightest analytic minds that this country has to offer.

Among other things, the NIE assessed:

- Al-Qa'ida is and will remain the most serious terrorist threat to the Homeland, as its central leadership continues to plan high-impact plots, while pushing others in extremist Sunni communities to mimic its efforts and to supplement its capabilities;
- Al-Qa'ida will intensify its efforts to put operatives in the United States;
- Al-Qa'ida's Homeland plotting is likely to continue to focus on prominent political, economic, and infrastructure targets with the goal of producing mass casualties, visually dramatic destruction, significant economic aftershocks, and/or fear among the US population.

I&A plays a critical role in providing vital intelligence to the owners and operators of our nation's critical infrastructure and key resources (CI/KR). In many respects, I&A's role is unique within the U.S. Intelligence Community (IC). We view our statutorily created

partnerships with the private sector as critical to the success of I&A, and critical to the success of DHS.

I&A's success in serving the private sector hinges upon our ability to share actionable, timely and relevant intelligence. Our CI/KR owners and operators deserve nothing less. The Department of Homeland Security has been a leader in establishing new approaches of information sharing - including sharing with the private sector. To be fully effective in these approaches, we must partner not only with the private sector, but with other parts of the intelligence community such as the FBI, and with other agencies within DHS and the Federal government.

Because of I&A's unique capabilities and department-wide responsibilities for assessing and analyzing all terrorism, homeland security, and related law enforcement and intelligence information received by the Department, Secretary Chertoff has designated I&A as the Department's executive agent for information sharing. In this capacity, we have created many mechanisms to bring together DHS' vast knowledge base and expertise to strengthen information sharing across the Department and, even more importantly, to share it with our external partners.

I would like to impart upon you today some of the information sharing efforts that DHS is leading, as well as describing some of our efforts with our Federal and intelligence community partners. The central theme you will see throughout is that we view the

private sector as a vital partner in our efforts, just as we view the FBI, and our state and local government partners.

As I noted above, the NIE assesses that Al-'Qa'ida's focus includes economic and infrastructure targets. A large number of these potential targets are owned and/or operated by our private sector partners. It is our shared goal - - our shared *responsibility* - - to ensure that the private sector has the intelligence it needs to better understand the threats they face, as well as the vulnerabilities that can be exploited by our enemies.

The private sector is more than just a customer of our intelligence products; they are a critical part of our production cycle. Given the size, diversity and complexity of the private sector, close cooperation with them is key to helping us understand the threats and vulnerabilities that exist. The private sector provides us with windows into understanding the threat based on their day-to-day observations and interactions across the country, helps us better understand their intelligence needs, and provides us with unique perspectives that help us fill intelligence gaps. We must therefore ensure a robust two-way flow of information between the Department and our private sector partners, as well as between our federal, state, local and tribal partners

Strengthening the Flow of Intelligence

DHS has focused a great deal of energy to ensure that our private sector partners receive the very best intelligence available. A linchpin of this effort is the Homeland Intelligence and Threat Analysis Center (HITRAC), a three-way partnership between our Office of Infrastructure Protection, I&A and the Private Sector. I will not delve deeply into how HITRAC functions, because we are fortunate that Ms. Smislova, HITRAC's Director, is

here to testify today. What I will say, however, is that HITRAC produces a variety of classified and unclassified intelligence products specifically tailored to serve private sector intelligence needs which is a unique effort within the Federal government. In addition to working with the DHS Office of Infrastructure Protection and its private sector partners, HITRAC closely coordinates its efforts with agencies such as the FBI, Transportation Security Administration, and the National Counter Terrorism Center.

Good intelligence is of little value unless it can be put into the hands of those who need it. I&A has established a strong Production Management (PM) division to ensure that our intelligence products, including those produced by HITRAC, are disseminated in a timely and efficient manner. Just as HITRAC's customers are diverse, so too must be our intelligence dissemination methods.

The I&A PM Division maintains comprehensive email dissemination lists, specifically designed to serve private sector partners at the unclassified level. Email distribution occurs using the Sector Coordinating Councils (SCCs), and when appropriate, Information Sharing and Analysis Centers (ISACs) list points of contact across the 17 CI/KR sectors : Chemical, Commercial Facilities, Dams, Emergency Services, Energy, Banking and Finance Agriculture and Food, Government Facilities, Public Health and Healthcare, National Monuments and Icons, Information Technology, Commercial Nuclear Reactors, Materials and Waste , Postal & Shipping, Telecommunications, Defense Industrial Base, Drinking Water and Water Treatment Facilities, and Transportation (including Aviation, Maritime, Railroad, Mass Transit, Highway),. In

addition to the email to the SCCs and ISACs, products are sent to the DHS National Infrastructure Coordinating Center (NICC) for posting to the corresponding unclassified HSIN – Critical Sectors where more private sector partners can view the products. Similarly, products classified at the Secret level are posted on the Homeland Secure Data Network (HSDN) - a network that is rapidly expanding, thanks in part to our efforts in the State and Local Fusion Center (SLFC) program.

However, sending emails and posting products is not enough. I&A's analysts also engage in extensive outreach efforts directly with private sector representatives, through HITRAC and the State and Local relationships. This effort generally is initiated by the State or locality itself and, is designed to push and pull information that directly relates to threats within a particular geographic region where, for example, that individual sector may be headquartered or maintain critical assets, such as plants or distribution centers. The response has been positive.

Moreover, state and local fusion centers (SLFCs) are increasingly helping to bridge the gap between sector specific threats and geographic threats, by such efforts as involving plant managers and small businesses - not just corporate offices – in fusion center activities. The private sector wants relationships built on trust. I&A is taking full advantage of the fact that many SLFC officials have already built strong private sector ties in their communities.

An example of this local dynamic is in Illinois, where the State Terrorism Intelligence Center (STIC) is using their State HSIN Portal as the primary tool for information sharing with the Private Sector. Major companies like Caterpillar, McDonald's, Cargill, and John Deere are part of this process, as well as smaller businesses that were identified through State incorporation listings.

Maryland is another fine example. Maryland has formed a Private Sector Council that has leaders from a number of Maryland based companies - big and small - who advise the Maryland Coordination and Analysis Center (MCAC), Maryland's primary fusion center, routinely on their information needs. Maryland's Private Sector Council has been formally recognized by the MCAC and they meet monthly to discuss threat-related issues within Maryland and the National Capital Region. While the main conduit in these examples is through the State Fusion Centers, both involve support from and frequent interaction with DHS.

The private sector needs a comprehensive understanding of the threats they face in order to develop mitigation strategies, to plan for continuity of operations in the event of an attack or disaster, and to protect its employees and assets. In addition to understanding credible threats, the private sector also needs to be aware of threats that lack credibility. I&A helps to add context to raw intelligence reporting to help the private sector better understand which threats are real and which ones don't necessarily require a response. This helps the private sector better manage its resources.

Write to Release – But Protect Privacy

DHS is participating in many federal efforts to further improve information sharing with the private sector. At the national level – DHS in conjunction with DOJ and the DNI, is creating the Interagency Threat Assessment and Coordination Group (ITACG). The ITACG is being established in response to the President's Guidelines for the creation and establishment of the Information Sharing Environment. The group will be part of the National Counterterrorism Center (NCTC) and will enable the development of intelligence reports on terrorist threats threat and related issues that represent a federally coordinated perspective and are tailored to meet the needs of state, local, and tribal governments. The ITAGC will be staffed by DHS and FBI personnel and will include representation from state and local entities. The coordination of counterterrorism information within NCTC ensures that products released from the Federal government will be of one voice and without delay. By including State and local partners as members of the ITAGC, the language appearing in federally disseminated products can be more focused or tailored in areas that are of greater interest and in a form that is most useful non-federal partners.

Similarly, there are many indisputably legitimate reasons for protecting sensitive information - even information that is unclassified. For example, information which we refer to generically as Sensitive but Unclassified (SBU) or Controlled Unclassified Information (CUI). Examples of CUI include personal information, information that could compromise ongoing law enforcement investigations or endanger witnesses,

information containing private sector proprietary information, and information containing private sector vulnerabilities and other security-related information that could be exploited by terrorists. Inappropriate disclosure of these types of information could cause injury to individuals, business, or government interests. We *must* balance the need to produce actionable intelligence, while protecting the liberties and rights of both individuals and businesses.

DHS understands the importance of protecting private sector proprietary information. We have created handling controls to facilitate information sharing in a protected manner. Within DHS, there are three such information-protection regimes -- "Protected Critical Infrastructure Information (PCII)," "Sensitive Security Information (SSI)," and the newly established "Chemical Vulnerability Information (CVI)." Congress mandated these categories of information be protected and DHS has promulgated regulations implementing these regimes. Each was specifically created to foster private sector confidence to increase their willingness to share with the federal government crucial homeland security-related information. To date, PCII and SSI have been successful in this regard and have been well-received by the private sector. Moreover, these designations are ready examples of how robust control of information can actually promote appropriate sharing.

Additionally, DHS is working with the Program Manager of the Information Sharing Environment (PM-ISE) and key information sharing stakeholders on the SBU Coordinating Committee to implement the President's direction in Presidential Guideline

3 , which, among other things, directs departments and agencies to provide recommendations to standardize sensitive but unclassified information handling and marking procedures so that federal agencies can more efficiently and effectively share SBU information with its many partners.

Conclusion

I appreciate the opportunity to share with you our efforts of sharing intelligence with the private sector. DHS recognizes the private sector not only as a critical customer, but a vital partner in protecting the homeland. I&A is dedicated to strengthening the information flow with our infrastructure threat analysis and the extensive distribution of theses products. DHS believes the private sector is an important part of our nation's intelligence cycle and actively engages them to help us understand real time requirements. We are building excellent private sector relationships through our State and local Fusion Centers. DHS is actively and collaboratively working with our Federal partners including DNI, FBI and others to ensure that the private sector can obtain the best available intelligence in a timely manner. We are dedicated to this important relationship and will continue to work to find new ways of strengthening it in support of homeland security.